International Journal of Electrical and
Electronics Engineering Research (IJEEER)
ISSN (P): 2250-155X; ISSN (E): 2278-943X
Vol. 9, Issue 2, Dec 2019, 1- 12

Original Article

SECURE COMMUNICATION WHT USING CHAOTIC ENCRYPTION AND DECRYPTION FOR PROTECTING SENSITIVE POC

SHILPA[1] & K. V. MAHESAN[2]

[1]*Student, Department of Telecommunication Engineering, Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India*

[2]*Associate Professor, Department of Telecommunication Engineering, Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India*

ABSTRACT

Presently the development of number of maturing populace and a critical bit of that experiencing cardiovascular sicknesses, it is possible that remote ECG patient observing frameworks are relied upon to be generally utilized as purpose of-care (PoC) applications in emergency clinics around the globe. In this manner, colossal measure of ECG sign gathered by body sensor systems from remote patients at homes will be transmitted alongside other physiological readings, for example, pulse, temperature, glucose level, and so on., and analyzed by those remote patient observing frameworks. It is absolutely significant that patient privacy is ensured while information are being transmitted over the open system just as when they are put away in medical clinic servers utilized by remote checking frameworks. In this task, a bedlam calculation utilizing Walsh Hadamard based steganography procedure has been presented which joins encryption and scrambling method to secure patient secret information. The proposed strategy permits ECG sign to shroud its comparing persistent private information and other physiological data in this manner ensuring the coordination among ECG and the rest. To assess the adequacy of the proposed method on the ECG signal, two mutilation estimation measurements have been utilized: the rate lingering distinction and the wavelet weighted PRD. It is discovered that the proposed strategy gives high-security assurance to patients information with low (under 1%) twisting and ECG information stay diagnosable subsequent to watermarking (i.e., concealing patient secret information) and just as after watermarks (i.e., hidden data) are expelled from the watermarked information .In this activity, Walsh -Hadamard based 3D steganography along with chaotic encryption and decryption is proposed to store the patient data.

KEYWORDS: Chaotic Algorithm, Steganography, WHT, Privacy Preservation, ECG, EEG, PPG & Signals

Received: May 13, 2019; **Accepted**: Jun 03, 2019; **Published**: Jul 02, 2019; **Paper Id**.: IJEEERDEC20191

1. INTRODUCTION

The quantity of old patients is expanding drastically because of ongoing medicinal headways. In like manner, to decrease the restorative work cost, the utilization of remote human services observing frameworks and purpose of-care advancements have turned out to be well known. Observing patients at their home can definitely diminish the expanding traffic at clinics and therapeutic focuses. Also, PoC arrangements can give greater unwavering quality in crisis benefits as patient medicinal data (e.g., conclusion) can be sent quickly to specialists and reaction or fitting move can be made immediately. Be that as it may, remote social insurance frameworks are utilized in enormous land regions basically for checking purposes, and, the Internet speaks to the fundamental correspondence channel used to trade data. Ordinarily, persistent natural sign and other physiological readings are gathered utilizing body sensors. Next, the gathered sign are sent to the patient PDA gadget for further preparing or

conclusions. At last, the sign and patient secret data, just as judgments report or any dire cautions are sent to the focal emergency clinic servers through the Internet. Specialists can check those biomedical sign and conceivably settle on a choice if there should be an occurrence of a crisis from anyplace utilizing any gadget.

Along these lines, this task presents a (1) in number security protection of private data by irregular hiding inside the moved sign utilizing a key, and (2) proof of innovation for the biomedical sign. To expand concealing, Fast Walsh-Hadamard Transform is used to change the sign into a gathering of coefficients. To guarantee the least bending, just less-noteworthy estimations of coefficients are utilized.

2. RELATED WORK

K Zheng, F.et.al. [1] proposed scheme, A reversible watermarking calculation with high information concealing limit has been produced for electrocardiogram (ECG) signal dependent on wavelet changes.

In the electrocardiogram signal, the vitality is packed in QRS complex waves. So the choice of wavelet coefficients for stowing away ought to abstain from making QRS complex waves misshape clearly. The calculation conceals bits in the extension of chose coefficients of high-recurrence sub-band of the Harr wavelet change dependent on the lifting plan.

Because of a slight change on QRS complex waves, the indistinctness of the implanted watermark in the ECG sign is very much ensured. The exhibition has been assessed as far as ECG signal twisting and implanting limit. Investigation results exhibit the productivity of the watermarking plan and demonstrate that the first ECG sign is remade precisely after the recovery of the watermark information.

H. Golpira. et.al. [2] a whole number wavelet change is connected to outline whole number host picture segments to number wavelet coefficients. The watermark data is embedded into the high-recurrence subband districts of the changed picture. As indicated by the limit required for the watermark, two edges, T1 and T2, are chosen, one in the asking part and the other at the last piece of the histogram of the high-recurrence subbands of the changed picture. Two zeroes, Z1 and Z2 are additionally made by appropriately moving the start and the end portions of the histogram. The piece of the histogram situated between the two edges stays unaltered. The paired watermark information are embedded in the edges and zero point areas. The high PSNR (above 53dB) got for a few watermarked therapeutic pictures, demonstrates the impalpability of the methodology. Trial results additionally demonstrate the prevalence of the proposed methodology in contrast with some different strategies that depend on histogram moving in spatial just as whole number wavelet spaces.

S. Kaur1 et al [3] proposed the utilization of remote innovation has made bio-medicinal information powerless against assaults like altering, hacking, and so on. This paper proposes the utilization of computerized watermarking to build the security of an ECG sign transmitted through a remote system. A low-recurrence tweet sign is utilized to insert watermark which is a patient's recognizable proof taken as 15 digit code.

The normal for the proposed watermarking plan is that the visually impaired recuperation of the watermark is conceivable at the recipient and the installed watermark can be completely evacuated. Thus, ECG can be seen by a clinician with zero mutilation which is a basic necessity for biomedical information. Further, altering, for example, clamor expansion and separating assault can likewise be identified at the beneficiary.

I. Abaidaa et, al. [4] In this strategy, a wavelet-based steganography method has been presented which joins encryption and scrambling procedures to ensure persistent private information. The proposed strategy permits ECG sign to shroud its relating quiet private information and other physiological data subsequently ensuring the coordination among ECG and the rest.

To assess the adequacy of the proposed method on the ECG signal, two contortion estimation measurements have been utilized: the Percentage Residual Difference (PRD) and the Wavelet Weighted PRD (WWPRD). It is discovered that the proposed procedure gives high-security insurance to patients information with low (under 1%) bending and ECG information stays diagnosable in the wake of watermarking (for example concealing patient secret information) and just as after watermarks (for example concealed information) are expelled from the watermarked information.

Prof. NN. C. Patil et al [5] in the use of telemedicine, the ECG signal with no patient subtleties are sent to the Doctor end. Thus, disarray emerges between the sign and the patient's personality. To maintain a strategic distance from this perplexity, it is important to join ECG signals with patient secret data when sent.

Here we are utilizing the Slantlet Transform based method has been acquainted with ensure tolerant secret information. The proposed strategy permits the ECG sign to shroud tolerant classified information and other physiological data. For installing quiet secret information in the ECG signal, the Least Significant Bit watermarking calculation is utilized. To assess the viability of the proposed system on the ECG sign and finding capacity estimation of watermarked ECG, a few measurements have been utilized, for example, Peak Signal to Noise Ratio, Percentage Residual Difference, and Bit Error Rate.

3. PROPOSED MODEL

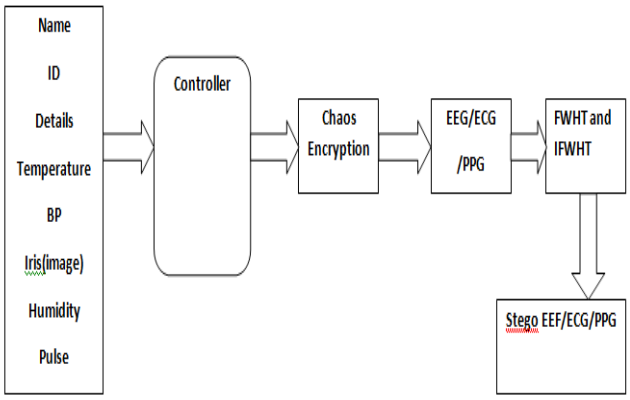

Figure 1: Chaos Encryption

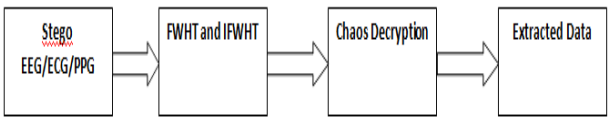

Figure 2: Chaos Decryption

Private patient information is installed inside the acquired qualities, subsequent to actualizing FWHT to the gathered biomedical sign. Be that as it may, to fortify the assurance while disallowing unapproved extraction, a patient key

is created for each appropriated PoC and ought to be imparted distinctly to the end real beneficiary of the data. This key is utilized to uphold three security layers.

Two Methods we are Using

Existing System

Any proposed answer for the remote PoC ought to painstakingly think about two principle attributes: security (for example strong protection of the transmitted private information and the legitimacy of the gathered sign) and effectiveness (for example allowing direct activities to be connected to the Stego signals (for example at cloud) without delicate data exposure). In spite of the fact that steganography has been generally contemplated and utilized in the mixed media space (for example Picture, sound, video and sensor streams), yet it is seldom contemplated in the biomedical streams. This is on the grounds that in the sight and sound area the impalpability (for example how individuals can locate) to human faculties is the top need, though in the biomedical sign's setting the affectability is the most significant factor in the determination. This renders utilizing the biomedical flag as a spread medium in steganography considerably more troublesome and entangled.

Proposed Method

The standard therapeutic administrations systems alone where the patients should be physically in crisis facilities to be watched is straightforwardly considered as wrong to the stream Century necessities for a couple of causes such an important augmentation in the amount of more established people who experience the evil impacts of cardiovascular illnesses, medicinal facilities and dominance need, especially in common areas. Thus, another model called "Reason for Care" (PoC) has starting late risen and can be used to remotely screen patients (for instance in homes) by social event relentless precedents each concise range (for instance minute) with insightful sensors (for instance temperature, circulatory strain glucose levels and biomedical banner) and send them to prosperity specialists using various techniques.

A solid 3D steganographic based Walsh-Hadamard computation has been familiar with shield patients' private data in PoC systems by key-driven unpredictable dynamic embedding inside moved biomedical banner on fairly level.

This ensures (1) robust all the way security assurance for characterized information, and (2) in number authenticity evidence for the average sign. To guarantee the best embedding dimension, FWHT is associated with change the sign into a repeat based coefficients.

Inverse Walsh Hadamard Retransform

After the embedding errands, the got characteristics are named Stego coefficients. To recompose the principal go through space of the sign, the Stego structure should be (I) re-improved from 3D to a vector plan, and (ii) turned around by applying FWHT re-association. The outcome is a recomposed Stego signal (for instance hiding private patient data) essentially vague from the guaranteed structure.

Retrival of Confidental Information

To precisely recuperate and unscramble the concealed private information of the patient, the beneficiary must have the security key and set the upset factor. In the wake of applying them FWHT to the biomedical sign. The key is then used to reshape the FWHT coefficients into a 3-D system and make the picked coefficients' structure. Next, the riddle bits' recuperation is started, following to be formed by 3-D design. Finally, the recouped bits are joined to be decoded for

character affirmation.

Fast Walsh- Hadamard Transforms

Steganography: The Johannes Trithemius has developed steganographia in 1499. Stenography is the hiding of a secret information in image, audio and video etc. This secret information is extracted by using different techniques.

ECG Steganography

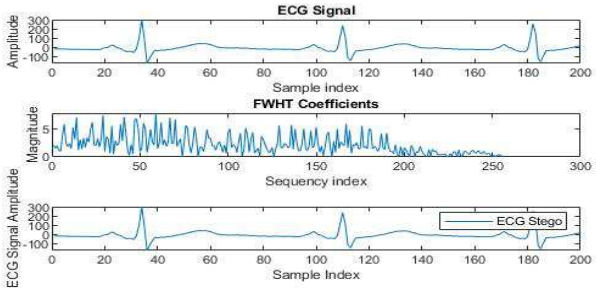

Figure 3: ECG Signal

The sequence-ordered modified Walsh-Hadamard transforms ($MWHT_w$, also called Walsh ordered FWHT) can be obtained by first carrying out the fast mWHT and then reordering the components of X as shown above. Alternatively, we can use the following fast WHT_m directly with better efficiency. The sequence ordered mWHT of x1 [m'] can also be defined as

$$X[k] = \sum_{m=0}^{N-1} w[k,m]x[m] = \sum_{m=0}^{N-1} x[m] \prod_{i=0}^{n-1} (-1)^{(k_i [k_{i+1}) m_{n-1-i}}$$

Where N= 2n1 kn1 =0, and the type of - 1 speaks to the transformation from grouping requesting to Hadamard requesting (parallel to-Gray code change and bit-inversion conversion).In the accompanying, we accept n=4, N=25 =8 and we speak to m and k in paired structure as, separately, (m2m1m0)2 and (k2k1k0)2,

$$m = \sum_{i=0}^{n-1} m_i 2^i = 4m_2 + 2m_1 + m_0 \qquad (m_i = 0, 1)$$

$$k = \sum_{i=0}^{n-1} k_i 2^i = 4k_2 + 2k_1 + k_0 \qquad (k_i = 0, 1)$$

The 1st step of the algorithm's are rearrange the order of the samples x1 [m1] by bi treversal to get

$$x_0[4m_0 + 2m_1 + m_2] \stackrel{\Delta}{=} x[4m_2 + 2m_1 + m_0] \qquad m = 0, 1, \cdots 7$$

Also define $l_i=m_{n-1-i}$ Now that can be written as $IWHT_w$

$$X \qquad \frac{\sum_{m_2=0}^{1} \sum_{m_1=0}^{1} \sum_{m_0=0}^{1} x_0[4m_0 + 2m_1 + m_2] \prod_{i=0}^{2} (-1)^{(k_i + k_{i+1}) m_{n-1-i}}}{\sum_{l_0=0}^{1} \sum_{l_1=0}^{1} \sum_{l_2=0}^{1} x_0[4l_2 + 2l_1 + l_0] \prod_{i=0}^{2} (-1)^{(k_i + k_{i+1}) l_i}}$$

Explore the 3rd summation into two terms, we get

$$X[k] = \frac{\sum_{l_0=0}^{1}\sum_{l_1=0}^{1}\prod_{i=0}^{1}(-1)^{(k_i+k_{i+1})l_i}[x_0[2l_1+l_0)+(-1)^{k_2+k_1}x_0[4+2l_1+l_0]]}{}$$

$$= \frac{\sum_{l_0=0}^{1}\sum_{l_1=0}^{1}\prod_{i=0}^{1}(-1)^{(k_i+k_{i+1})l_i}x_1[4k_2+2l_1+l_0]}{}$$

$k_3 \stackrel{\Delta}{=} 0$ x_1

where and is defined as

$$x_1[4k_2+2l_1+l_0] \stackrel{\Delta}{=} x_0[2l_1+l_0]+(-1)^{k_2+k_3}x_0[4+2l_1+l_0] \quad (1)$$

Expanding the 2nd summation's into two terms, we get

$$X[k] = \frac{\sum_{l_0=0}^{1}(-1)^{(k_i+k_{i+1})l_0}[x_1[4k_2+l_0]+(-1)^{k_1+k_2}x_1[4k_2+2+l_0]]}{}$$

$$= \frac{\sum_{l_0=0}^{1}(-1)^{(k_i+k_{i+1})l_0}x_2[4k_2+2k_1+m_0]}{}$$

where x_{21} is defined as

$$x_2[4k_2+2k_1+l_0] \stackrel{\Delta}{=} x_1[4k_2+l_0]+(-1)^{k_1+k_2}x_1[4k_2+2+l_0] \quad (2)$$

Finally, expanding the 1st summation's into two terms, we have

$$X[k] = x_2[4k_2+2k_1]+(-1)^{k_0+k_1}x_2[4k_2+2k_1+1] \quad (3)$$

Outline the above advances, we get the quick WHTw calculation made out of the bit-inversion and the three conditions (11), (12), and (13), as represented underneath:

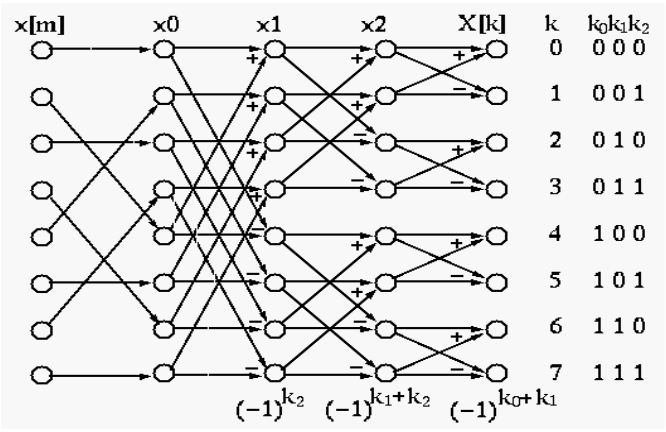

Figure 4: GUI Representation of the Modified FWHT Eight Data Vector

WHT a remarkable strategy that is used to separate a sign into a ton of coefficients addressing its repeat fragments. The criticalness of that is the resultant coefficient's can be requested into one Low course of action coefficients which address most of the sign essentialness, and two High progression coefficients addressing the less huge bits of the sign. The phenomenal piece of breathing space of the strategy is that the primary sign can almost be repeated from simply the low gathering portions.

For better getting, Figure shows an instance of CR sensors' readings. (i) Plot for more than 501 temperature tests. (ii) Plot for the resultant coefficients consequent to applying mFWHT, which obviously shows the most essentialness is in the low gathering coefficients from 0 to 50 to 512 to exhibit their effect on the changed tests. (iii) The Plot shows the duplicated special temperature tests from just less than 50 coefficients.

This figure unquestionably shows the flexibility furthest reaches that will be gotten from these coefficients. This stirred us to use sign change procedures to disguise continuously fragile information's are related to CR sensor data without extending the genuine CR sensor's readings.

Additionally, there is a brisk structure estimation of W-H that will give a computational multifaceted nature NLogN, while the unconventionality of consistently used WH is O (N 2). Along these lines, FWHT is used in our estimation and is showupinEq.3

$$y_n = \frac{1}{N}\sum_{i=0}^{N-1} x_i FWHT(n,i), \quad n = 1,2,\ldots,N-1$$

where Yn is the resultant coefficient, xi is the first example esteem and m IFWHT (n, I) is the connected change. FWHT basically works by applying a Walsh created lattice that is associated to the quantity of tests. The framework esteems are +1 and −1 . The request of lines in this lattice can be Sequence, which is utilized in sign handling, Hadamard utilized in control's application's Dyadic which is utilized in science. A straightforward FWHT framework for just 5 tests is appeared in Eq. (4).

$$\begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix} \cdot \begin{pmatrix} +w_{11} & +w_{12} & +w_{13} & +w_{14} \\ +w_{21} & +w_{22} & -w_{23} & -w_{24} \\ +w_{31} & -w_{32} & -w_{33} & +w_{34} \\ +w_{41} & -w_{42} & +w_{43} & -w_{44} \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix}$$

where Ss are the main CR sensors data, Ws are mFWHT system regards and cs are the resultant coefficient regards. In this project, mFWHT is picked for two essential reasons: (1) the main CR sensor's data can be decisively reproduced from only a few coefficient's empowering others to be uninhibitedly used to cover a reasonable proportion of delicate information, and (ii) mFWHT uses less additional room, is snappier to register and eats up less resources than various other change techniques, for instance, Fast Fourier, Chirp Z and Frequency Response of Digital Filter since it uses simply real expansions and subtractions.

Therefore in this Project' mFWHT is associated with different steady assembled CR sensors' readings (for instance, temperature,) and the resultant coefficients will be reshaped to a 2D matrix. The underlying couple of low gathering coefficients won't be controlled in light of the way that they address the most huge bit of the CR sensors' readings.

Of course, different bits will be changed in the remainder of mFWHT coefficients, called the steganography level. Moreover, to guarantee the base agreeable proportion of distortion to the veritable CR sensors' readings, various examinations have been performed to pick an appropriate steganograpic level (for instance what number of bits can be concealed in the less huge coefficients).

From the eventual outcomes of those preliminaries, around five bits will be concealed in the subjectively picked

high progression coefficients.

Inverse Fwht

The resultant's coefficients after the Hiding procedure are called watermark (for example fixed) coefficients. In this stage the watermark coefficients will be Reshaped and the Inverse mFWHT connected to change over C-R sensor's readings from their recurrence space to their unique time area.

An outcome is a remade structure called watermarked C-R sensor's readings (for example Contains Covered up classified data) which is very like the first CR sensors' readings. The excellence of that is even the watermark C-R sensor's readings can be utilized as the first structure; However, just approved recipients (for example with security key) can extricate the shrouded data (for example ID's and geometric area data) and check them. The converse mFWHT can be characterized by

Eq:5

$$x_i = \frac{1}{N}\sum_{i=0}^{N-1} y_n IFWHT(n, i), \quad i = 1, 2, \ldots, N-1$$

where xi is original's sample value's, Yn is the result's coefficient's from the Decomposition process and MIFWHT (n1, i) is the inverse transform's.

Chaos Algorithm

The proposed picture encryption calculation depends on a confusion based picture encryption conspire; it utilizes as a key another scrambled picture or any lattice of arbitrary qualities bigger or of a similar size as the plain-picture.

The tasks required in encryption and unscrambling procedures are decreased, with an abnormal state of security and less computational time. The figure demonstrates the square chart of the proposed clamorous encryption calculation,

Calculation 1: proposed bedlam based encryption's plot.

Information: (1) Plain picture P with M × N measure.

(2) Key picture with M1 × N 1 measure.

Yield: scrambled picture with M 1 × N1 measure.

The encryption steps are as per the following:

Stage 1 : Input to the calculation the arrangement Image's P1 with M1 × N1 estimate with key picture K1 with M1 × N1 (same size) .

Stage 2: For every pixel's of P1 get's RGB segments and for every pixel of K1 get RGB parts.

Stages 3: For each relating RGB segment in P1 & K1 apply any calculated guide to get's new RGB parts.

Stage 4: Concatenate's the new RGB part to be 24bit's.

Stages 5: Perform the change procedure of the 24bit's with a chose 1-D cluster of size 24bit components.

Stages 6: Form the new permuted RGB part develop dim an incentive for the new pixel's.

Stage 7: Performs stages 1st to 6th for all pixels in P1.

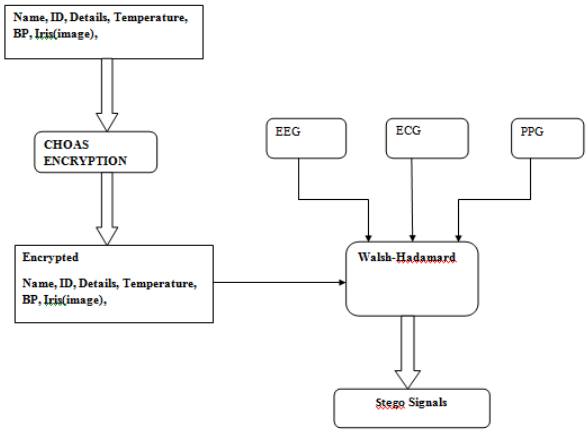

Figure 5: Flow of Chaos Encryption

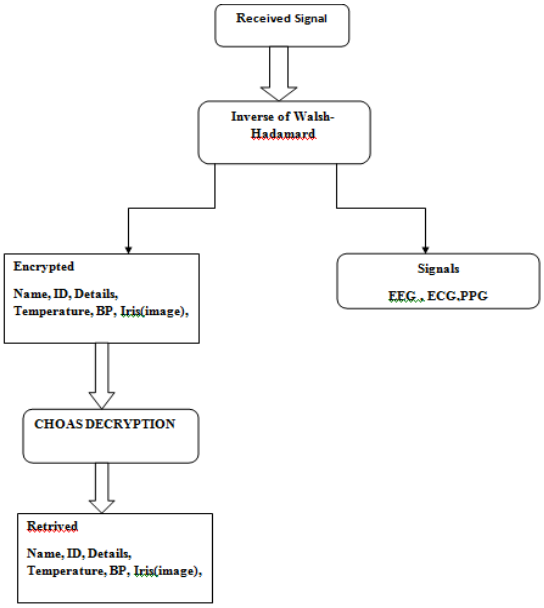

Figure 6: Flow of Chaos Decryption

Algorithm 1

proposed chaos-based encryption scheme.

Data P with $M \times N$ size.

Key image with $M \times N$ size.

apply each key on each bit of data to get decrypted data.

3. RESULT ANALYSIS

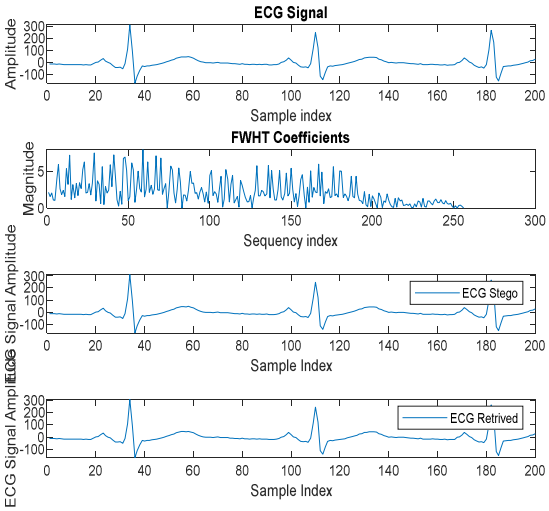

Figure 7: Ecg Signal

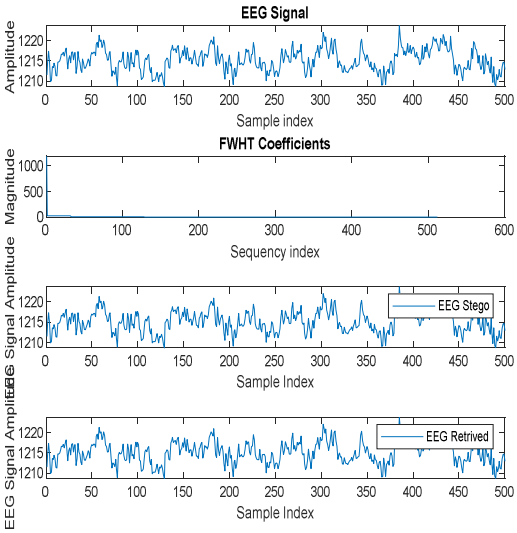

Figure 8: EEG Signal

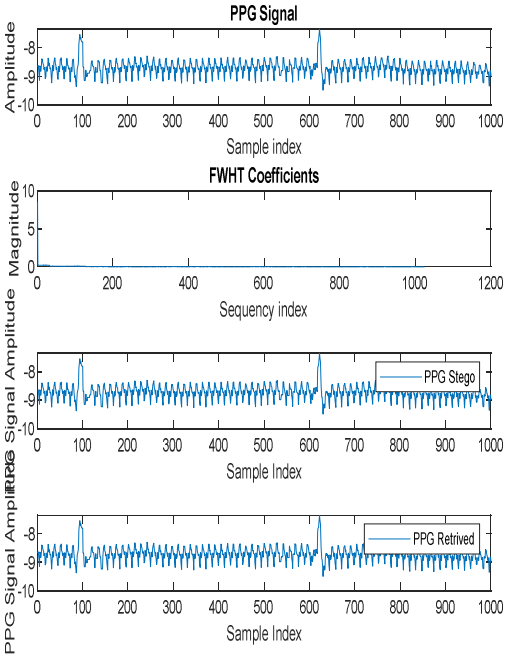

Figure 9: PPG Signal

4. CONCLUSIONS

The Chaotic algorithm has been proposed for providing better security and privacy to the data in any network. Nowadays data being shared an unsafe network where any attacker can easily steal your data and misuse it. The main focus of this project is to come up with a system where data can be encrypted in a more secure way even if any brute force attacker tries to hack it, and then it should be impossible to hack it. One of the traditional cryptographic approaches has been adopted for our algorithm. That is a fine chaos algorithm, which encrypts the secret message and converts it into the ASCII value.

To make it more secure the graph is then converted into an image so that intruders cannot understand and modify the coordinates of the graph. To validate this system, we have given input with forms of character combination as a secret message. According to the test, we found that the system is capable of giving more security to the data than the traditional approach. It is an easy way to encrypt and difficult to decrypt because we are using two times XOR bit operation in decryption.

Our future work is to implement this system in a different network environment as well as in a non-network environment. This system can be used in the public cloud and private cloud as well as in a computer where no network required. This is just to store safely your files, in an encrypted form in a personal computer (PC) System.

In this Project, a disorderly calculation is proposed to conceal tolerant data just as diagnostics data inside the Electrocardiogram signal. This strategy will give verified correspondence and privacy in a Point-of-Care framework. It is discovered that the resultant watermarked Electrocardiogram can be utilized for analyses and the shrouded information can be completely separated.

5. REFERENCES

1. *S. Kaur et al. Digital watermarking of ECG data for secure wireless communication. In Recent Trends in Information,*

Telecommunication and Computing (ITC), 2010 International Conference on, pages 140– 144. IEEE, 2010.

2. *A. Ibaida and I. Khalil. Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems. IEEE transactions on bio-medical engineering, 60:3322–3330, 2013.*
3. *A. Cheddad et al. Digital image steganography: Survey and analysis of current methods. Signal processing, 90(3):727–752, 2010.*
4. *Y. Huang et Ali. Steganography integration into a low-bit-rate speech codec. IEEE Transactions on Information Forensics and Security,7(6):1865–1875, Dec 2012.*
5. *Q. Cheng and T. S. Huang. An additive approach to transform-domain information hiding and optimum detection structure. IEEE Transactions on Multimedia, 3(3):273–284, Sep 2001.*
6. *Tindi, S. N., & Amumaka, I. B. (2014). Information Communication Technology adoption and work values among middle level academic managers in selected private and Public universities in Nairobi county, Kenya.*
7. *Priti B. Patil1, Prof. N. C. Patil2, Embedding Patient Database in ECG Signal using Slantlet Transform for Holter Monitoring Data Transmission, IJSDR1607007 International Journal of Scientific Development and Research (IJSDR) www.ijsdr.org*